UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/127,767	07/31/98	PATEL S	2925-0161P

002292 WM31/0511
BIRCH STEWART KOLASCH & BIRCH
PO BOX 747
FALLS CHURCH VA 22040-0747

EXAMINER	
KABAKOFF, S	
ART UNIT	PAPER NUMBER
2132	4

DATE MAILED: 05/11/01

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	**Application No.** 09/127,767	**Applicant(s)** PATEL, SARVAR	
	Examiner Steve Kabakoff	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 March 2001* .

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)

16) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

17) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 5 .

18) □ Interview Summary (PTO-413) Paper No(s). _____ .

19) □ Notice of Informal Patent Application (PTO-152)

20) □ Other: .

DETAILED ACTION

1. Claims 1-22 have been examined.

Response to Arguments

2. Applicant's arguments filed March 1, 2001 (paper number 4) have been fully considered but they are not persuasive and therefore the original claim rejections have been maintained in the current Office Action.

On pages 2-4 of the applicant's reply filed March 1, 2001 (paper number 4), the Examiner identified two main points in which the applicant believes the claimed inventions are patentably distinct from the prior art of record:

(i) "section 10.3.1 [in Menezes et al] teaches that various time variant parameters may be used in identification protocols... it is nowhere suggested in Menezes that each specific type of time variant parameter is 'interchangeable.' It is further respectfully submitted that the applied reference, at best, may suggest that one of advanced skill in the art *could* eventually be led to the invention, however, this does not amount to establish a *prima facie* case of obviousness."

The Examiner does not find this argument convincing since Menezes et al explicitly teaches time variant parameters are "used in identification protocols to counteract replay and interleaving attacks (see 10.5), to provide uniqueness or timeliness guarantees, and to prevent certain chosen-text attacks" (beginning of section 10.3.1 on page 397 of Menezes et al). Thus, each of the time variant parameters disclosed in Menezes et al is used for the same purpose in identification and authentication protocols, such as the protocols in the claimed inventions.

It appears the applicant admits one of advanced skill could be led to his invention based on the teachings of the cited portions in Menezes et al, and the Examiner believes Menezes et al would also be a reference for one of ordinary skill in the art at the time of the invention who worked in the field of cryptographic protocols.

(ii) "It should be noted that a MAC algorithm [in the SKID3 protocol taught in Menezes et al] amounts to a keyed hash algorithm and does not amount to a teaching or suggestion of the key cryptographic function as recited, for example, in claim 1."

The applicant's argument is based on an alleged difference between the claimed "key cryptographic function" and a "keyed hash algorithm." This argument is not convincing since a hash function is a type of cryptographic function. Although the SKID3 protocol relied on by the Examiner in the claim rejections uses a keyed one-way function (a.k.a "keyed hash algorithm" or a "keyed MAC"), such a function by definition is a keyed cryptographic function as in the claimed inventions.

The Examiner notes that the applicants define a key cryptographic function at the bottom of page 3 of the specification: "A keyed cryptographic function (KCF) is a type of cryptographic function that operates based on a key; for instance, a cryptographic function which operates on two or more arguments (i.e., inputs) wherein one of the arguments is the key." The keyed one-way function in the SKID3 protocol meets the criteria for a KCF defined by the applicant in his specification.

Furthermore, at the top of page 402 in Menezes et al, an authentication protocol similar to SKID3 is disclosed using a more generic keyed cryptographic function called "E_K." In the middle of page 402 Menezes et al explicitly equates the keyed one-way function in SKID3 with a more generic keyed cryptographic function E_K: "the encryption function E_K is replaced by a MAC algorithm h_K."

On pages 4-7 of the applicant's reply filed March 1, 2001 (paper number 4), the applicant presents separate "Independent Grounds for Allowability." However, most of the analysis on these pages comprises one or both of the above-identified arguments. But the following additional points were also presented:

(iii) "We disagree and submit that Menezes fails to teach or suggest establishing a second key."

In response, the Examiner notes the claim language does not require the "second key" to be a different key from the "first key." Furthermore, establishing a key "*based*" on first and second challenges does not imply the first and second challenges are used to *derive* the key. Therefore, as stated in the original claim rejections, the key "K" in the SKID3 protocol in Menezes et al is a shared key between two parties implementing an authentication protocol based on two challenges r_A and r_B. In other words, the teachings in Menezes et al read on the current claim language.

(iv) "It is respectfully submitted that a teaching that information is included regarding a form of a challenge in an identifier does not amount to a teaching of a type of authentication protocol."

The Examiner admits information regarding a form of a challenge does not amount to a teaching of the type of authentication protocol being used as the applicant attests. However, claim 7 teaches type data *indicating* a type of protocol being performed, not *identifying* the type of protocol being performed. Although a subtle distinction, it is enough so the claim language reads on the SKID3 protocol in Menezes et al.

The claim rejections stated: "a type of authentication protocol depends on the form of the challenges," and the Examiner believes information regarding the form of a challenge is indicative of the type of protocol being implemented. In other words, the applicants do not argue that Menezes et al teach inclusion of the form of a challenge in the SKID3 authentication protocol, and the Examiner argues information regarding the form of challenges in Menezes et al is data indicating the type of authentication protocol being used, as set forth in claim 7.

(v) "The Examiner asserts that the choice of 64 bit or greater counter value would have been an obvious design choice. Applicant respectfully disagrees... Further, it is merely asserted that initializing a counter with a random number is standard practice."

The Examiner maintains the choice of a 64 bit or greater counter value would have been an obvious design choice for implementing the SKID3 authentication protocol taught in Menezes et al when counter values up to 2^{64} are required.

Page 399 of Menezes et al states: "The simplest policy is that a sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received." However, the Examiner stated "it was standard practice in the art of initializing a counter to start at some random offset value to add an extra layer cryptographic security against potential reverse engineering of the authentication system." Of course, using such an offset would not be the "simplest" method as stated in Menezes et al, but it would be make it more difficult for a hacker/interloper to guess what counter value is being utilized by an authentication protocol.

To reinforce the Examiner's original statement a quick search was conducted and the Bantz et al (US 5515439) reference cited at the end of this Office Action is submitted simply as proof that it was known at the time of the invention to offset a counter value to an arbitrary initial value in an authentication protocol to make eavesdropping and replaying attacks from intruders more difficult (ie, see abstract). As mentioned previously, Menezes et al also disclose the use of time-variant counter values as a means for preventing replay attacks in authentication protocols such as in SKID3 and in the claimed inventions.

Claim Objections

3. The Examiner has removed the objection to claim 5 in response to the amendment filed March 1, 2001 (paper number 4).

4. Applicant is reminded of the new 37 CFR 121(c) rules for submitting amended claims; applicants are now required to submit a clean copy of the pending claims as well as a marked up copy of those claims that are amended in future correspondences.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes et al (Handbook of Applied Cryptography).

Claim 1: The claimed invention is directed to a method for mutually authenticating a first and second party. Such mutual authentication systems were known in the art at the time of the invention, and the Examiner will refer to SKID3 disclosed on page 402 of Menezes et al as merely one example.

The claimed invention teaches (a) receiving a random number, (b) incrementing a count value, (c) generating a response by performing a key cryptographic function (KCF) on the received random number and count value, (d) transferring the count value and the generated response, (e) receiving another response being a result of performing a KCF on the transferred count value, and (f) verifying the response received in step e.

In SKID3 disclosed on page 402 of Menezes et al, party A (a) receives a random value r_B, (b) creates a new value r_A, (c) generates a response by performing a KCF on the received value r_B and the newly created value r_A, (d) transfers r_A and the generated response, (e) receives another response being a result of performing a KCF on the transferred value r_A, and (f) verifies the response received in step e.

By direct comparison of SKID3 and the claimed invention, SKID3 only differs from the claimed invention in regards to using a value r_A instead of a "count value" as disclosed in the claim.

However, pages 397-400 of Menezes et al disclose interchangeability in authentication protocols of random numbers, such as r_A, with sequence numbers, such as the count value in claim 1. In particular, Menezes et al disclose three different types of numbers used in authentication protocols to prevent "replay" attacks: (i) Random numbers, (ii) Sequence numbers, and (iii) Timestamps. The Examiner notes that one of ordinary skill in the art at the time of the invention would have known replay attacks were used to subvert challenge-response authentication protocols, and therefore would have been familiar with choosing one of the three above options.

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use a counter value in place of random number r_A in the SKID3 authentication protocol taught in Menezes et al, since pages 397-400 of Menezes et al disclose random numbers, sequence numbers, serial numbers, counter values, and timestamps were all viable options known for preventing replay attacks in authentication protocols such as SKID3.

Claim 2: The claimed invention teaches generating a first key from a root key. It was well known in the art at the time of the invention to generate a secondary key using an A-key as a root key; in fact, on lines 20-26 of page 3 of the specification the applicant describes such a prior art system in regards to applicant's Fig. 1 (identified as prior art). Thus, it would have been obvious to one of ordinary skill in the art at the time of the invention to use an A-key to generate key K in the SKID3 protocol of Menezes et al since this was a well known and often implemented method for effectively generating a cryptographic key in the art.

Claim 3: The claimed invention includes an identifier in the response created in step (c) of claim 1. Menezes et al disclose including identification information "B" in the corresponding response (page 402) of the SKID3 authentication protocol.

Claim 4: The claimed invention teaches establishing a second key based on the first and second challenges described in claim 1. In SKID3 disclosed by Menezes et al, a cryptographic key K is generated based on the protocol encrypting challenges r_A and r_B using the generated key K.

Claim 5: The claimed invention teaches the challenge in step (a) of claim 1 is a global challenge. Clearly, SKID3 in Menezes et al could be used for authenticating a plurality of mobile units when r_B is broadcast globally from a single base unit. Page 3 of the applicant's specification describes a prior art authentication system comprising a base station and corresponding mobile stations that would have been an obvious choice to use a well known authentication protocol such as SKID3 described in Menezes et al.

Thus it would have been obvious to one of ordinary skill in the art at the time of the invention to implement an authentication protocol such as SKID3 using global challenges when implementing authentication systems comprising a single base station and a plurality of mobile stations as described in the prior art authentication system on page 3 of the specification.

Claim 6: The claimed invention teaches a wireless system. Applying an authentication protocol to a wireless system was known in the art at the time of the invention as evidenced by the admitted prior art system discussed on page 3 of the specification. Clearly, one of ordinary skill in the art at the time of the invention would know a standard authentication protocol such as SKID3 could be implemented in a wireless environment such as that described in the admitted prior art system in the specification.

Claim 7: The claimed invention teaches including type data indicating a type of protocol being performed in the response generated in step (c) of claim 1. Menezes et al disclose identifiers included in the generated responses ("A" and "B" on page 402), where the identifiers allow a recipient to verify the identifier as his/her own and optionally embed additional random numbers in the identifier or include information regarding the form of the challenges (see bottom of page 401 of Menezes et al—although the text relied on in Menezes et al does not directly refer to the SKID3 protocol, the identifiers described by Menezes et al on page 401 are the same as those in the SKID3 protocol disclosed on page 402).

Since Menezes et al teaches including information regarding "the form of the challenges" in identifiers included in a generated response, it would have been obvious to one of ordinary skill in the art at the time of the invention that including information pertaining to the form of challenges as disclosed at the bottom of page 401 of Menezes et al is the same as including protocol information as taught in claim 7 since a type of authentication protocol depends on the form of the challenges.

Claim 8: The claimed invention contains the same limitations as previously rejected claims 3 and 7 and is rejected for the same reasons.

Claim 9: The claimed invention contains the same limitations as previously rejected claim 4 and is rejected for the same reasons.

Claim 10: The claimed invention teaches the second key is one of shared secret data and a session key. In SKID3 disclosed by Menezes et al, cryptographic key K corresponds to the second key in the claimed invention where K is clearly a shared key since both A and B have access to it. Therefore, key K in SKID3 taught in Menezes et al is shared secret data between A and B.

Claim 11: The claimed invention teaches incrementing the count value using a bit counter greater than 64 bits which was initialized using a random number. Page 399 in Menezes et al discloses using a counter value in lieu of a random number to prevent replay attacks against an authentication protocol such as SKID3 (see previous discussion of claim 1), but Menezes et al does not explicitly teach a specific size or initialization procedure for generating a counter value.

The choice of a 64 bit or greater counter value would have been an obvious design choice for implementing the SKID3 authentication protocol taught in Menezes et al when counter values up to 2^{64} are required. Furthermore, it was standard practice in the art of initializing a counter to start at some random offset value to add an extra layer cryptographic security against potential reverse engineering of the authentication system.

Claims 12-22: The claimed inventions contain the same limitations as previously rejected claims 1-11 except from the point of view of the first party instead of from the point of view of the second party.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Bantz et al (US 5515439)

Patel (US 6014085)

Dent et al (US 5559886)

Dent et al (US 5594795)

Michener et al (US 5351293)

Fischer (US 5659617)

Bruwer et al (US 5841866)

9. Any inquiry conceming this communication or earlier communications from the examiner should be directed to Steve Kabakoff whose telephone number is (703) 306-4153. The examiner can normally be reached on 8:30am to 6:00pm except every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-0040 for regular communications and (703) 305-9051 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

SK
SEK
May 10, 2001

TOD SWANN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100